UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,385	06/19/2002	Tobias Martin	520.1007	3809

7278 7590 07/11/2007

DARBY & DARBY P.C.
P.O. BOX 770
Church Street Station
New York, NY 10008-0770

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
07/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/049,385	MARTIN ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 2 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 May 2007*.

2a)☐ This action is **FINAL**. 2b)☐ This action is non-final.

3)☒ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3-18* is/are pending in the application.

4a) Of the above claim(s) *3 and 4* is/are withdrawn from consideration.

5)☒ Claim(s) *5,7-10 and 12-18* is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☒ Claim(s) *6 and 11* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 02 May 2007 has been entered.

2. By the above submission, Claims 5, 7, 8, and 13-15 have been amended. New Claims 16-18 have been added. No claims have been canceled. Claims 3 and 4 were previously withdrawn from further consideration as drawn to a nonelected invention. Claims 5-18 are currently under consideration in the present application.

Election/Restrictions

3. Except as further noted below, this application is in condition for allowance except for the presence of claims 3 and 4 directed to an invention non-elected without traverse. Accordingly, claims 3 and 4 have been cancelled.

Specification

4. The disclosure is objected to because of the following informalities:

The specification does not appear to contain a section with a "Brief Description of the Drawings" as required by 37 CFR 1.74, nor does there appear to be any reference in the specification to the drawing Figure whatsoever. See MPEP § 608.01(f).

Appropriate correction is required. Applicant's cooperation is requested in correcting any other errors of which applicant may become aware in the specification.

Claim Objections

5. Claims 6 and 11 are objected to because of the following informalities:

Claim 6 recites the limitation "the transmission key is known to subscriber T_j". It appears that the phrase should instead read "the transmission key is known to each subscriber T_j" for increased clarity.

Similarly, Claim 11 recites the limitation "the transmission key is known to a respective subscriber T_j"; it appears that this should instead read "the transmission key is known to each respective subscriber T_j" for increased clarity.

Appropriate correction is required.

Allowable Subject Matter

6. Claims 5, 7-10, and 12-18 are allowed.

7. Claims 6 and 11 would be allowable if rewritten to overcome the objections set forth in this Office action.

8. The following is an examiner's statement of reasons for allowance:

Each of independent Claims 5, 7, and 13 are directed to methods for establishing a common encryption key within a group of subscribers. The methods each include subscribers calculating messages using an element of a group and a respective random number, sending these messages to each other subscriber, encrypting the received messages at a first coordinating subscriber to generate pairwise transmission keys between the coordinating subscriber and each other subscriber, sending messages to each subscriber encrypted with the respective transmission key, and using all of the received messages or derivations thereof to calculate a common key, which is then used to encrypt and send messages between members of the group. Various cited prior art describes conference keying processes. For example, Ingemarsson et al, "A Conference Key Distribution System", discloses a system for establishing a key in a group derived from Diffie Hellman key distribution, and Laih et al, "On the Design of Conference Key Distribution Systems for the Broadcasting Networks, analyzes several group key establishment protocols and discloses a system for establishing a group key based on a threshold scheme. Both Ingemarsson and Laih were cited in the Office action mailed 10 August 2006. However, while these references describe general

conference keying schemes, they do not disclose the specifics of the claimed methods. Further, Steiner et al, "Diffie-Hellman Key Distribution Extended to Group Communication" describes several group key establishment protocols, including the Burmester/Desmedt Protocol (see page 35, section 4.2), which also has two rounds like the claimed methods; however, this protocol differs from the claimed methods in the contents of the actual messages sent, and further does not use a coordinating first subscriber. Finally, Yasinsac et al, "A Family of Protocols for Group Key Generation in Ad Hoc Networks", does disclose a group key agreement protocol that has two rounds and uses a coordinating first subscriber (see page 3); however, Yasinsac does not qualify as prior art for the present application.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Caronni et al, US Patent 6195751, discloses a group key establishment protocol for secure multicasting.

b. Srivastava, US Patent 6987855, discloses a key exchange protocol within broadcast groups based on Diffie-Hellman.

10. This application is in condition for allowance except for the following formal matters:

The disclosure is objected to under 37 CFR 1.74, and Claims 6 and 11 are objected to for informalities as detailed above.

Prosecution on the merits is closed in accordance with the practice under *Ex parte Quayle*, 25 USPQ 74, 453 O.G. 213, (Comm'r Pat. 1935).

A shortened statutory period for reply to this action is set to expire **TWO MONTHS** from the mailing date of this letter.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER